UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. - JIAQIANG XU, Defendant.	S1 16 Cr. 10 (KMK)

THE GOVERNMENT'S MEMORANDUM OF LAW IN RESPONSE TO DEFENDANT'S MOTIONS (1) TO SUPPRESS HIS POST-ARREST STATEMENT, (2) TO DISMISS THE INDICTMENT, AND (3) TO COMPEL DISCOVERY

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the United States of America

Benjamin Allee
Ilan Graff
Shane Stansbury
Assistant United States Attorneys
Of Counsel

The Government respectfully submits this memorandum in response to the defendant's motions (1) to suppress his post-arrest statements (Docket No. 20); (2) to dismiss the indictment (Docket No. 21); and (3) to compel discovery (Docket No. 22). For the reasons set forth below, the motions should be denied. The motions to dismiss the indictment and to compel discovery are without merit, and the motion to suppress his post-arrest statement is moot because the Government is not seeking to offer the statement in its direct case.

BACKGROUND

The defendant is charged in Superseding Indictment S1 16 Cr. 10 (the "Indictment") in six counts. In the first three counts, the defendant is charged with economic espionage crimes: (1) stealing and attempting to steal a trade secret, intending or knowing that it would benefit a foreign government or agency thereof, in violation of Title 18, United States Code, Sections 1831(a)(1) and (a)(4) (Count One); (2) distributing, and attempting to distribute, a stolen trade secret, intending or knowing that it would benefit a foreign government or agency thereof, in violation of Title 18, United States Code, Sections 1831(a)(2) and (a)(4) (Count Two); and (3) possessing, and attempting to possess, a stolen trade secret, intending or knowing that it would benefit a foreign government or agency thereof, in violation of Title 18, United States Code, Sections 1831(a)(3) and (a)(4) (Count Three). In the last three counts, the defendant is charged with trade-secrets crimes: (4) theft and attempted theft of a trade secret, in violation of Title 18, United States Code, Section 1832(a)(1) and (a)(4) (Count Four); (5) distribution and attempted distribution of a stolen trade secret, in violation of Title 18, United States Code, Section 1832(a)(2) (Count Five); and (6) possession and attempted possession of a stolen trade secret, in violation of Title 18, United States Code, Section 1832(a)(3) (Count Six).

The Government anticipates proving at trial, through the testimony of witnesses and introduction of documents and other physical evidence, that the defendant stole, distributed, and possessed valuable intellectual property of a United States company (the "Victim Company"), intending to use it for his own profit and to benefit an agency of the People's Republic of China (the "PRC"). The intellectual property was the Victim Company's source code, which was a trade secret (the "Proprietary Source Code"). (See Compl., ¶ 5.) The Victim Company created and developed the Proprietary Source Code to produce valuable proprietary software that is used by government agencies and private corporations to facilitate faster computer performance and coordinate work among multiple servers (the "Proprietary Software"). (Compl., ¶¶ 3-6.)

The proof at trial will show that the Victim Company stored the Proprietary Source Code on servers in the United States. The defendant was a former employee of the Victim Company who had worked in its China Branch, and was well aware that the Proprietary Source Code was the confidential intellectual property of the Victim Company. (Compl., ¶¶ 7(a)-(d).) The defendant stole the Proprietary Source Code from the Victim Company. (Compl., ¶¶ 10-12, 15-20.) He then used the stolen Proprietary Source Code for his own benefit and with the intent to benefit the PRC's National Health and Family Planning Commission ("NHFPC"), going so far as to create a startup company that sold products created using the Proprietary Source Code.

The proof at trial will further show how the defendant was caught. As described in the Complaint, for approximately one year, the defendant communicated with two individuals —who represented themselves as an entrepreneur and project manager, respectively, of a technology company, but who in fact were undercover FBI agents located in the United States—

about the Proprietary Source Code. (Compl., ¶¶ 8-20.) The communications were by email, Skype, and in person. The defendant's purpose in engaging in the communications with the undercover agents was to attempt to use the Proprietary Source Code, and his ability to create software with it, for his own profit. During the communications, the defendant admitted, among other things, that:

- he had the Victim Company's Proprietary Source Code;
- he had obtained multiple versions of it, including even after he left the Victim Company;
- he had a startup company that used the Proprietary Source Code to create software that it sold;
- the overwhelming majority of the Proprietary Source Code is not open source; and
- he modified the Proprietary Source Code for the specific purpose of concealing that it was the Victim Company's.

(Compl., ¶¶ 12-20). The defendant also made numerous other inculpatory statements, such as the fact that he used the Proprietary Source Code for the benefit of the NHFPC.

During the communications, the defendant also provided items to the undercover agents to demonstrate the truth of his claims. For example, he emailed the U.S.-based agents a portion of the Proprietary Source Code. (Compl., ¶¶ 10-11.) He also uploaded, to a U.S.-based server, software for the agents that he had created using the Proprietary Source Code. (Compl., ¶¶ 16-18.) And, after traveling to the United States with the Proprietary Source Code, the defendant met with the undercover agents in White Plains, New York. He then showed the agents items on his computer regarding his interactions with the NHFPC. Thereafter, when the FBI arrested the defendant, they found on his computer additional evidence, including the

Proprietary Source Code, and additional documents corroborating the defendant's admissions to the agents.

DISCUSSION

I. The Defendant's Motion To Dismiss for Lack of Jurisdiction Should Be Denied

The defendant argues that four of the six charges returned by the grand jury should be dismissed because the Court lacks "jurisdiction." (Def. Br., at 5-8).[1] He notes that the statutes under which he is charged in the Indictment, 18 U.S.C. §§ 1831 and 1832, which criminalize economic espionage and theft of trade secrets, respectively, apply to conduct occurring outside of the United States only if (1) the defendant is a citizen or permanent resident of the United States, or (2) "an act in furtherance of the offense was committed in the United States." 18 U.S.C. § 1837. The defendant asserts that, as he is not a United States citizen or permanent resident, he cannot be guilty of the crimes charged in Counts One, Two, Four, and Five, because "even if [he] stole the source code and converted it to his own use, he did so while in China." (Def. Br., at 6.) On this basis he moves for dismissal of the Indictment for lack of jurisdiction.

The defendant's motion should be denied, because, as set forth below: (1) the Court has subject matter jurisdiction over the case because the Indictment charges violations of federal law; (2) the defendant's challenge goes to the merits of the case and in particular the sufficiency of the Government's proof, and must be decided upon the evidence at trial by a jury (and/or the Court under Rule 29 standards); and (3) in any event, the Government's proof at trial will be more than sufficient to show that the defendant committed the charged crimes within the territorial reach of the applicable statutes. The Economic Espionage Act explicitly criminalizes

[1] "Def. Br.," as referenced in this section, refers to the defendant's brief in support of his motion to dismiss the Indictment. See Docket No. 21.

conduct occurring outside the United States when an act "in furtherance of" the offense is committed in the United States, and the evidence at trial will show that the defendant committed numerous acts in furtherance of the charged offenses both in the United States and China.

First, to the extent that the defendant is arguing that the Court lacks *subject matter* jurisdiction—that is, jurisdiction over the case—the issue does not turn on the arguments the defendant makes regarding the geography of his criminal conduct. Rather, this Court has jurisdiction over a criminal case when a grand jury returns an indictment charging a defendant with violating federal criminal laws. *See* 18 U.S.C. § 3231 ("The district courts of the United States shall have original jurisdiction . . . of all offenses against the laws of the United States."); *United States* v. *Cotton*, 535 U.S. 625, 630 (2002); *United States* v. *Yousef*, 750 F.3d 254, 259-60 (2d Cir.) (2014); *United States* v. *Rubin*, 743 F.3d 31, 38-39 (2d Cir. 2014). "[T]o invoke a district court's jurisdiction, an indictment need only allege that a defendant committed a federal criminal offense at a stated time and place in terms plainly tracking the language of the relevant statute." *Rubin*, 743 F.3d at 38; *see United States* v. *Williams*, 341 U.S. 58, 65 (1951) (rejecting argument for lack of jurisdiction because the case involved an alleged violation of federal law); *United States* v. *Manuel*, 371 F. Supp. 2d 404, 408-09 (S.D.N.Y. 2005) (Lynch, J.) ("In the first place, the [defendant's] argument misstates the question. A court has subject matter jurisdiction over a case, not over a person, and the Court plainly has jurisdiction over the case, because the indictment charged a violation of federal law."); *see, e.g.*, *Yousef*, 750 F.3d at 259 (citing *United States* v. *Shellef*, 507 F.3d 82, 96 (2d Cir. 2007) ("The district court had jurisdiction over the prosecution of [defendants] pursuant to 18 U.S.C. § 3231 because they were charged with violating federal criminal laws."); *United States* v. *Keigue*, 318 F.3d 437, 439 (2d Cir.2003) (similar)). Here, the Indictment charges the defendant in six counts with violations of federal law and properly tracks the language of the relevant statutes. This Court, therefore, has subject matter jurisdiction.

Second, rather than contesting the Court's subject matter jurisdiction, the defendant appears instead to be arguing that his conduct, with respect to Counts One, Two, Four, and Five, falls outside the territorial reach of the economic espionage and trade secrets statutes. (Def. Br., at 7 ("Absent evidence that Defendant Xu committed some act in furtherance of the stealing of the code or the copying of the code in the United States, this Court lacks jurisdiction to prosecute [him] . . . . The [Economic Espionage Act] simply does not provide jurisdiction to prosecute someone for coming to the United States after having stolen or copied a trade secret.")). That is, the defendant appears to argue not that the Court does not have jurisdiction over the case, but rather that the Government will be unable to prove a jurisdictional element of the offenses charged. *See United States* v. *Griffith*, 284 F.3d 338, 346 (2d Cir. 2002) (discussing as-applied constitutional challenges to criminal statutes and how the presence of "jurisdictional elements," such as interstate transportation requirements in statutes regarding child pornography, assure that a particular defendant's conduct is proved to be within the reach of Congress's legislative power); *see also Torres* v. *Lynch*, 136 S. Ct. 1619, 1624 (2016) ("The substantive elements primarily define the behavior that the statute calls a violation of federal law. . . . The jurisdictional element, by contrast, ties the substantive offense (here, arson) to one of Congress's constitutional powers (here, its authority over interstate commerce), thus spelling out the warrant for Congress to legislate."); *United States* v. *Tinoco*, 304 F.3d 1088, 1110 (11th Cir. 2002) (citing *United States* v. *Krilich*, 209 F.3d 968, 972 (7th Cir. 2000)) (explaining that the jurisdictional element "is not really a matter of the court's subject matter jurisdiction," but instead is "inserted into the statute to provide Congress with substantive authority under Article I of the Constitution, or to bring the statute into compliance with due process restraints").[2]

To the extent the defendant is making this argument, his motion should be denied as premature and without procedural basis. Although a challenge to the Court's "jurisdiction" may be brought at any time, *see* Fed. R. Crim. Proc. 12(b)(2), the defendant's argument based on the location of his criminal conduct is a *merits* question that cannot be resolved at this pretrial stage of the case, any more than a challenge to a substantive element could be made at this stage of the case. *See Yousef*, 750 F.3d at 260 (rejecting defendant's challenge based on the "territorial nexus" of his conduct, noting that "[t]he defendant's contention that in fact certain of the statutory elements are lacking goes to the merits of the prosecution, not to the jurisdiction of the court to entertain the case or to punish the defendant if all of the alleged elements are proven." (internal quotation marks, alterations, citation omitted)); *see also Morrison* v. *National Australia Bank Ltd*., 561 U.S. 247, 254 (2010) (clarifying that a challenge to the extraterritorial reach of a statute—in that case, Section 10(b) of the Securities Exchange Act—did not raise a question of subject matter jurisdiction but rather "what conduct § 10(b) prohibits, which is a merits question"); *Lamar* v. *United States*, 240 U.S. 60, 64 (1916) (noting that the defendant's argument that his conduct fell outside of the conduct proscribed by the statute was not a jurisdictional challenge but rather went "only to the merits of the case").

---

[2] The jurisdictional element in this case can be likened to such requirements in an extraterritorially applicable narcotics statute, where Congress has made clear the statute's extraterritorial reach while ensuring the presence of a U.S. nexus. *See, e.g.*, 21 U.S.C. § 959(b) (making it a crime for "any United States citizen on board any aircraft" or for "any person on board an aircraft owned by a United States citizen or registered in the United States" to manufacture or distribute, or possess with intent to distribute, a controlled substance); *United States* v. *Epskamp*, No. 15-2028-cr, 2016 WL 4150900, at *8-*9 (2d Cir. Aug. 5, 2016) (describing such language in § 959(b) as a jurisdictional element, and holding that although the Government had to prove that the aircraft in question was registered in the United States, the Government did not have to prove the defendant's knowledge as to that element).

Rather, that question—whether the Government's proof is sufficient to show that, with respect to Counts One, Two, Four, and Five, the defendant's conduct occurred within the scope of the applicable statutes—is a question for the jury to decide at trial. *See United States* v. *Alfonso*, 143 F.3d 772, 776-77 (2d Cir. 1998) (reversing district court's pretrial dismissal of indictment in Hobbs Act robbery case based on insufficient showing that the jurisdictional element would be met, where there had not even been a full proffer of the evidence that would be presented at trial, and instructing that "'[w]hen a question of federal subject matter jurisdiction is intermeshed with questions going to the merits, the issue should be determined at trial'") (quoting *United States* v. *Ayarza-Garcia*, 819 F.2d 1043, 1048 (11th Cir. 1987)); *see also* Fed. R. Crim. P. 12(b)(1) (restricting pretrial motions to "any defense, objection, or request *that the court can determine without a trial on the merits*") (emphasis added).[3] And to the extent that the defendant seeks to argue that the evidence of the territorial nexus of his conduct is insufficient for any rational jury to find him guilty, the proper recourse is for the defendant to bring a motion pursuant to Rule 29. *See* Fed. R. Crim. P. 29; *Ayarza-Garcia*, 819 F.2d at 1048-49. But a Rule 29 motion must be made at trial or thereafter, after the Government rests, and the Court's decision on the motion requires analysis not merely of the Indictment, or the relevant criminal statutes, but of the Government's case-in-chief, viewing the evidence together as a whole and drawing all inferences in favor of the Government. *See United States* v. *Reyes*, 302 F.3d 48, 53

[3] To be sure, there may be circumstances where a statute's territorial reach may implicate the Government's authority to prosecute the case and therefore may appropriately be resolved prior to trial, such as where the defendant contends that the statute in question does not apply to extraterritorial conduct or that applying the statute to the defendant's extraterritorial conduct would violate due process. *See Yousef*, 750 F.3d at 260 ("A court's power to hear a case does not, of course, conclusively establish the government's authority to prosecute it. Our jurisprudence is replete with limitations on the exercise of that authority, whether by virtue of constitutional provisions, like the Due Process Clause, or judicially created doctrines, like the presumption against extraterritoriality.") The defendant cannot and does not make any such contention here.

(2d Cir. 2002) (view evidence as a whole on Rule 29 motion); *United States* v. *Aleskerova,* 300 F.3d 286, 292 (2d Cir. 2002) (draw inferences in the Government's favor on Rule 29 motion).

Third, although the defendant's challenge is premature and should be denied on that basis alone, his contention that his conduct did not come within the territorial reach of the applicable statutes—which is based on nothing other than an unsupported factual assertion in defense counsel's brief—is simply wrong. The economic-espionage and trade-secrets crimes with which the defendant is charged were enacted in the Economic Espionage Act in 1996. Pub. L. 104-294, Tit. I, § 101(a), 110 Stat. 3488 (1996). Congress had determined that there was a gap in criminal statutes prohibiting the theft of trade secrets, which "created substantial problems for American businesses, as the value of proprietary information is almost entirely dependent on its being kept secret. At the same time, the growing use of computer technology in all phases of business made such information easier to steal . . ." Sand, *Modern Federal Jury Instr*., Instr. 49A-1, Comment (citing legislative history). "As a result, Congress determined that the protection of proprietary economic information was warranted, and enacted [the Economic Espionage Act] as a comprehensive tool for government to combat the theft of trade secrets." *Id.*

As part of the Economic Espionage Act, Congress enacted a specific provision regarding extraterritoriality, codified at 18 U.S.C. § 1837. This provision, as noted above, makes explicit on its face that the crimes of economic espionage and theft of trade secrets include conduct occurring outside of the United States if, among other things, "an act *in furtherance of* the offense was committed in the United States." 18 U.S.C. § 1837(2) (emphasis added); *compare, e.g*., *United States* v. *Naranjo*, 14 F.3d 145, 147 (2d Cir. 1994) (describing similarly the standard for venue: "venue is proper in any district in which an overt act in furtherance of the [crime] was committed").

Here, the Government anticipates that the proof at trial will show that the defendant's conduct, both inside and outside of the United States, came within the territorial reach of the applicable statutes in multiple ways. Among other things, the trade-secret material consisting of the Proprietary Source Code that the defendant accessed, possessed, stole, distributed, was located and kept by the U.S.-based Victim Company on servers *in the United States*. The defendant stole multiple versions of the Proprietary Source Code from the Victim Company, including even after he no longer worked at the Victim Company.[4] The defendant engaged in numerous other acts "in furtherance of" the charged crimes, including by communicating with individuals in the United States about the stolen Proprietary Source Code, and by concealing the stolen code and traveling with it to the United States in an attempt to profit from it. The evidence at trial will amply demonstrate that as to each the six counts in which the defendant is charged, his charged conduct falls clearly within the territorial reach of the Economic Espionage Act.

---

[4] The defendant, ignoring the plain language of 18 U.S.C. § 1837, suggests that the statute requires any act in furtherance of the offense to occur at some particular point in time (*e.g.*, at the point at which the Proprietary Source Code was physically obtained or transferred) or while defendant *himself* was physically located in the United States. (Def. Br., at 5-7). But that is not what the plain language of the statute says, and indeed it runs contrary to the extraterritoriality provision's stated purpose, *i.e.*, to capture "conduct occurring outside the United States." 18 U.S.C. § 1837. Thus, the defendant's theft of Proprietary Source Code from servers in the United States, even while the defendant is physically located elsewhere, plainly falls within the scope of the statute, as are the defendant's numerous other actions in the United States "in furtherance of" the charged crimes. Indeed, it is, of course, well established in diverse contexts that computer crimes extend well beyond the location of the keyboard at which a particular defendant is sitting. *See, e.g.*, *United States* v. *Rowe*, 414 F.3d 271, 277-80 (2d Cir. 2005) (holding that venue for a defendant who posted an internet advertisement to trade child pornography from a computer in Kentucky was proper in the Southern District of New York, since the advertisement had been viewed in this district); *United States* v. *Johnson*, 510 F.3d 521, 524-26 (4th Cir. 2007) (Wilkinson, J.) (finding electronic transmission of false documents from Las Vegas-based company through computer servers in Alexandria, Virginia, sufficient to support venue for securities prosecution in the Eastern District of Virginia).

II. The Defendant's Motion To Compel Discovery Should Be Denied

The defendant moves to compel production of any report, summary, document or information showing that (1) code the defendant provided was not the Proprietary Source Code, (2) some portion of the Proprietary Source Code is open source, and (3) the defendant told undercover agents that he was not willing to sell the Proprietary Source Code. The defendant also seeks (4) any report, summary or comment by the FBI or the United States Attorney's Office suggesting that there was some concern during the investigation of this matter as to whether the defendant had trouble communicating with FBI agents.

Pursuant to its discovery obligations, the Government has provided the defense in this case with video recordings, audio recordings, emails and other communications, expert reports, FBI records, Victim Company records, search warrant returns including emails and forensic images of hardware (and the related search warrants and affidavits), investigative reports, draft transcripts, surveillance photos, and other documents. In addition, in response to the defense's recent requests and motions, the Government has supplemented its discovery with additional investigative reports and attachments that would otherwise be produced at a later date pursuant to 18 U.S.C. § 3500.

Of particular relevance to the defendant's motion to compel, among the discovery the defense has been provided are copies of the email, Skype, and in-person communications between the defendant and the undercover agents, all of which were written or recorded. The defendant has also been provided draft transcripts of the in-person meetings. The Government has provided reports of the expert who has reviewed the source code the defendant provided to the FBI and that was recovered from the defendant's computer, and who has concluded that it is the Proprietary Source Code. In addition, as noted above, on the request of defense counsel, the Government also produced certain FBI reports regarding the investigation.

As to the defendant's first request—for production of any report, summary, document or information showing that code the defendant provided was not the Proprietary Source Code—the Government is not aware of the existence of any item responsive to this request. In its brief, the defense refers to documents concerning the defendant's provision of source code by email in March 2015, suggesting that such documents would fit within this request. These documents do not fall within this request, because they do not show that the code the defendant provided was not the Proprietary Source Code, but the Government produced them to the defense nevertheless. The motion to compel such disclosure should therefore be denied.

As to the defendant's second request—for production of any report, summary, document or information showing that some portion of the Proprietary Source Code is open source—the Government has provided information showing that a small portion of the Proprietary Source Code—which in its entirety is enormous—is open source. The motion to compel such disclosure should therefore be denied. The Government notes, however, that this information is publicly available, is already known to the defense, and has none of the importance the defense attempts to attach to it. Indeed, during the investigation in recorded conversations with an undercover agent (the "UC"), the defendant himself described that he knew the Proprietary Source Code was not open source:

> Undercover Agent ("UC"): Well that's what I was wondering because I know there's open source versions of [the Proprietary Software] out there and I was just wondering why we don't just go with something like that?
>
> Defendant: Open source?
>
> UC: Yeah, open source [Proprietary Software].

Defendant: Uh no, that's not open source, that's just one part of the code is open source.

UC: Oh it's just a small piece?

Defendant: That is for . . . , yes. That is for [a particular portion], that's, that's open source, but most of the part is not, yeah.

As to the defendant's third request—for production of any report, summary, document or information showing that the defendant told undercover agents that he was not willing to sell the Proprietary Source Code—the Government has produced the defendant's communications with the undercover agents. The Government opposes any request at this time for internal reports or information about those communications, which is expressly foreclosed by Rule 16(a)(2) of the Federal Rules of Criminal Procedure.

As to the defendant's fourth request—for production of any report, summary or comment by the FBI or the United States Attorney's Office suggesting that there was some concern during the investigation of this matter as to whether the defendant had trouble communicating with FBI agents—the Government opposes this request. As with the third request, the fourth request seeks items foreclosed from discovery by Rule 16(a)(2). Moreover, the Government has produced the communications themselves to the defense, which communications, in the Government's view, flatly disprove any proffered defense theory premised on a purported language barrier. The motion should therefore be denied.

III. The Defendant's Motion To Suppress His Post-Arrest Statement Should Be Denied as Moot

The defendant moves to suppress his post-arrest statement to Special Agents of the FBI, arguing that his *Miranda* waiver in connection with his post-arrest statement was not knowing and voluntary. The defendant argues, without submitting any affidavit or declaration to this effect, that a Chinese/English language barrier existed during the interview, such that he did not understand his rights.

The Government does not currently intend to offer the defendant's post-arrest statement as part of its case-in-chief at trial. The defendant's motion is therefore moot, and should be denied.[5]

CONCLUSION

For the reasons set forth above, the Government respectfully submits that the defendant's motions to dismiss the Indictment and to compel discovery should be denied, and the motion to suppress his post-arrest statement should be denied as moot.

Dated: White Plains, New York
September 16, 2016

Respectfully submitted,

PREET BHARARA
United States Attorney

By: /s/ Benjamin Allee
Benjamin Allee/Ilan Graff/Shane Stansbury
Assistant United States Attorneys
(914) 993-1962/(212) 637-2296/2641

[5] To be clear, the Government reserves the right to offer the post-arrest statements for other permissible purposes, including for impeachment purposes should the defendant choose to testify. Such use would be permissible even were the impeachment evidence illegally or improperly obtained (which, in this case, it was not). *See, e.g., Harris* v. *New York*, 401 U.S. 222, 225 (1971) (permitting Government to impeach defendant using incriminating yet voluntary and reliable statements elicited in violation of *Miranda*); *Walder* v. *United States*, 347 U.S. 62, 74 (1954) (permitting introduction of physical evidence obtained through an illegal search to undermine the credibility of the defendant).